Effective discrimination using key update

Patent number: CN1256599

Publication date: 2000-06-14

Inventor: BERENTZVIG ADAM L (US); BRATHWAITE KALOS E (US)

Applicant: LUCENT TECHNOLOGIES INC (US)

Classification:

- international: ***H04L9/32;*** *H04Q7/32; H04Q7/38;* **H04L9/32;** H04Q7/32; H04Q7/38; (IPC1-7): H04Q7/20; H04L9/00

- european: H04L9/32

Application number: CN19990123679 19991108

Priority number(s): US19980188818 19981109

Also published as:

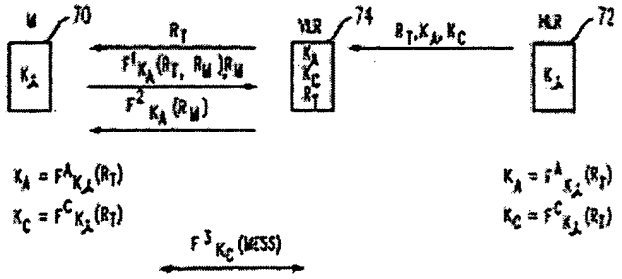
- E P1001570 (A2)
- J P2000269959 (A)
- E P1001570 (A3)
- CA 2282942 (A1)
- B R9905142 (A)

Abstract not available for CN1256599

Abstract of corresponding document: **EP1001570**

A more efficient method for performing authentication is provided by using an authentication challenge transmitted to a terminal to provide the terminal with the information to calculate authentication and cipher key values. As a result, a separate communication is not required to provide the terminal with key values. A visiting authentication center obtains a random value RT, an authentication key value KA and a cipher key value KC from a home authentication center. The visiting authentication center then transmits the random number RT to the terminal to update the terminal's authentication key and cipher key values, and to challenge the terminal as part of an authentication process. The terminal uses RT to calculate the authentication key value KA and the cipher key value KC, and to respond to the visiting authentication center's challenge. In addition, the authentication key value is used to verify the visiting network's response to the terminal's authentication challenge to the network.

FIG 5



[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
H04Q 7/20
H04L 9/00

[12]发明专利申请公开说明书

[21]申请号 99123679.3

[43]公开日 2000年6月14日

[11]公开号 CN 1256599A

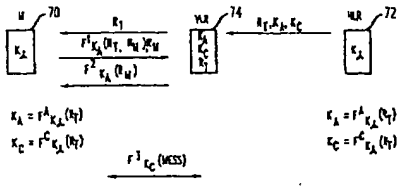
[22]申请日 1999.11.8 [21]申请号 99123679.3
[30]优先权
[32]1998.11.9 [33]US [31]09/188,818
[71]申请人 朗迅科技公司
地址 美国新泽西州
[72]发明人 亚当·L·贝伦兹韦格
卡洛斯·E·布拉思韦特
[74]专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 蒋世迅

权利要求书3页 说明书6页 附图页数3页

[54]发明名称 采用密钥更新的有效鉴证

[57]摘要

通过使用发射到终端的鉴证询问以提供给终端计算鉴证和密码本值的信息来提供一种实现鉴证的更有效的方法。因此，不需要分开的通讯来提供给终端密钥值。访问鉴证中心从归属鉴证中心获得随机值R_T、鉴证密钥值K_A和密码本值K_C。访问鉴证中心随后发射随机数R_T到终端以更新终端的鉴证密钥和密码本值，并且询问终端作为鉴证过程的一部分。终端使用R_T计算鉴证密钥值K_A和密码本值K_C，并且响应访问鉴证中心的询问。



ISSN1008-4274

权 利 要 求 书

1. 一种鉴证方法，包括步骤：

发射第一值到终端；

从具有至少第一响应值的终端接收响应，这里第一响应值是使用第一值的至少第一部分作为输入和第一密钥值作为密钥输入的第一密码函数输出的至少一部分，第一密钥值是使用第一值的至少第二部分作为输入和第二密钥值作为密钥输入的第二密码函数输出的至少一部分；以及

验证第一响应值等于期望的第一响应值。

2. 如权利要求 1 所述的方法，其中第二密钥值与终端有关。

3. 如权利要求 1 所述的方法，其中第一和第二密码函数是相同的。

4. 如权利要求 1 所述的方法，其中第一和第二部分是相同的。

5. 如权利要求 1 所述的方法，其中该响应具有第二响应值并且还包括发射第二值到终端的步骤，这里第二值是使用第二响应值的至少一部分作为输入和第三密钥值作为密钥输入的第三密码函数输出的至少一部分。

6. 一种鉴证方法，包括步骤：

发射第一值到终端；

从具有至少第一响应值和第二响应值的终端接收响应，这里第一响应值是使用第一值的至少第一部分和第二响应值的至少第一部分作为输入和第一密钥值作为密钥输入的第一密码函数输出的至少一部分，第一密钥值是使用第一值的至少第二部分作为输入和第二密钥值作为密钥输入的第二密码函数输出的至少一部分；以及

验证第一响应值等于期望的第一响应值。

7. 如权利要求 6 所述的方法，其中第二密钥值与终端有关。

8. 如权利要求 6 所述的方法，其中第一和第二密码函数是相同的。

9. 如权利要求 6 所述的方法，其中第一值的第一和第二部分是相同的。

10. 如权利要求 6 所述的方法，还包括发射第二值到终端的步骤，这里第二值是使用第二响应值的至少第二部分作为输入和第三密钥值作为密钥输入的第三密码函数输出的至少一部分。

11. 一种鉴证方法，包括步骤：

接收第一值；以及

发射具有至少第一响应值的响应，这里第一响应值是使用第一值的至少第一部分作为输入和第一密钥值作为密钥输入的第一密码函数输出的至少一部分，第一密钥值是使用第一值的至少第二部分作为输入和第二密钥值作为密钥输入的第二密码函数的输出的至少一部分。

12. 如权利要求 11 所述的方法，其中第一和第二密码函数是相同的。

13. 如权利要求 11 所述的方法，其中第一和第二部分是相同的。

14. 如权利要求 11 所述的方法，其中该响应具有第二响应值并且还包括接收第二值的步骤，这里第二值是使用第二响应值的至少一部分作为输入和第三密钥值作为密钥输入的第三密码函数的输出的至少一部分。

15. 如权利要求 14 所述的方法，还包括验证第二值等于期望的第二值的步骤。

16. 一种鉴证方法，包括步骤：

接收第一值；以及

发射具有至少第一响应值和第二响应值的响应，这里第一响应值是使用第一值的至少第一部分和第二响应值的至少第一部分作为输入和第一密钥值作为密钥输入的第一密码函数输出的至少一部分，该第一密钥值是使用第一值的至少第二部分作为输入和第二密钥值作为密钥输入的第二密码函数输出的至少一部分。

17. 如权利要求 16 所述的方法，其中第一和第二密码函数是相同的。

18. 如权利要求 16 所述的方法，其中第一值的第一和第二部分是相同的。

19. 如权利要求 16 所述的方法，还包括接收第二值的步骤，这里第二值是使用第二响应值的至少一部分作为输入和第三密钥值作为密钥输入的第三密码函数输出的至少一部分。

20. 如权利要求 19 所述的方法，还包括验证第二值等于期望的第二值的步骤。

说　　明　　书

采用密钥更新的有效鉴证

本发明涉及通讯，尤其涉及无线通讯系统中通讯各方的鉴证。

图 1 说明一个基站 10，它的相关小区 12 以及小区 12 内的移动站 14. 当移动站 14 第一次登记或试图与基站 10 通讯时，基站 10 在允许移动站接入通讯网络之前鉴证或验证移动站的身份。当移动站 14 在一个网络而不是它的归属网络时，这被称为在一个访问网络中。归属网络是由服务提供者控制的网络，该服务提供者与移动站终端的所有者订立合同以提供无线通讯服务。如果移动站工作在一个访问通讯网络，则基站 10 对移动站的鉴证将包括与移动站归属网络的鉴证中心 16 的通讯。在图 1 的例子中，移动站 14 在一个访问网络中。因此，移动站 14 的鉴证包括与移动站归属网络的鉴证中心 16 的通讯。当移动站 14 试图进入访问者网络时，基站 10 与访问通讯网络的鉴证中心 18 通讯。鉴证中心 18 由移动站或终端识别符如移动站 14 的电话号码确定移动站 14 登记在使用归属鉴证中心 16 的网络。随后访问鉴证中心 18 经过如 IS41 信令网 20 的网络与归属鉴证中心 16 通讯。归属鉴证中心 16 随后进入对于移动站 14 具有登记入口的归属位置寄存器 22。归属位置寄存器 22 可以通过一个识别符如移动站电话号码与终端或移动站联系起来。包含在归属位置寄存器中的信息用于产生加密密钥和其他信息随后提供给访问者鉴证中心 18 的访问者位置寄存器 24. 来自访问者位置寄存器 24 的信息随后用于提供给基站 10 发射到移动站 14 的信息，使得移动站 14 能够响应并且因此鉴证为一个有资格接受通讯服务的移动站。

图 2 说明在 GSM 无线网络中使用的鉴证过程。在这种情况下，移动站和归属位置寄存器都包含密钥 K_i。当移动站请求接入访问网络时，访问鉴证中心接触归属鉴证中心以接收变量 RAND、SRES 和 K_C。归属鉴证中心使用来自与该移动站有关的归属位置寄存器的值

K_i以产生值 SRES 和 K_C。通过使用具有随机数 RAND 作为输入和值 K_i作为密钥输入的称为 A3 的密码函数来计算值 SRES. 以相同的方式，通过使用具有 RAND 作为输入和值 K_i作为密钥输入的密码函数 A8 来计算密码本 K_C。这些值随后传送到访问鉴证中心的访问者位置寄存器。访问鉴证中心随后通过发射随机数 RAND 到移动站询问移动站。移动站随后以归属鉴证中心相同的计算方式计算值 SRES 和 K_C。然后移动站发射值 SRES 到访问鉴证中心，这里访问鉴证中心将从移动站接收的 SRES 与从归属鉴证中心接收的 SRES 相比较。如果这些值匹配，则允许移动站接入访问网络。如果移动站和访问网络之间的其他通讯要被加密，则使用具有被加密的消息作为输入和具有等于值 K_C的密钥输入的 A5 密码函数加密这些通讯。密码函数 A3、A5 和 A8 在本领域是公知的并且被 GSM 标准推荐。在 GSM 系统中，每当移动站进入访问网络中的新的呼叫，则执行包括与归属鉴证中心通讯的这个鉴证过程。

图 3a 和 3b 说明了用于 IS41 依从网络的鉴证过程。IS41 依从网络的例子是使用 AMPS、TDMA 或 CDMA 协议的网络。在这个系统中，移动站和归属位置寄存器都包含一个称为 AKEY 的秘密值。当移动站请求接入访问网络时，访问网络鉴证中心请求来自归属鉴证中心的数据。在实际鉴证过程可以开始之前，通过提供给移动站和访问者位置寄存器将用于通讯和鉴证的加密算法一起使用的密钥实现密钥更新。使用如移动站电话号码的标识符定位与移动站有关的归属位置寄存器并且存储在归属位置寄存器的 AKEY 用于产生将发射到访问者位置寄存器的数据。计算的值是 SSDA（共享秘密数据 A）和 SSDB（共享秘密数据 B）值。通过使用随机数 R_s作为输入和值 AKEY 作为密钥输入实现 CAVE 算法来计算这些值。CAVE 算法在本领域是公知的并且在 IS41 标准中作了规定。归属鉴证中心随后传送值 R_s、SSDA 和 SSDB 到访问网络的访问者位置寄存器。访问网络随后更新共享秘密数据（SSDA 和 SSDB），通过发射 R_s到移动站将由移动站使用这些数据。移动站随后以归属鉴证中心相同的计算

方式计算 SSDA 和 SSDB。既然移动站和访问者位置寄存器都包含 SSDA 和 SSDB 值，则鉴证过程可以进行。

图 3b 说明在移动站和访问位置寄存器已经接收到密钥 SSDA 和 SSDB 之后，如何在访问网络内鉴证移动站，访问鉴证中心通过发送随机数 R_N 到移动站询问移动站。这时，移动站和访问鉴证中心计算值 AUTHR，这里 AUTHR 等于使用随机数 R_N 作为输入和 SSDA 值作为密钥输入的 CAVE 算法的输出。移动站随后发射计算的值 AUTHR 到访问鉴证中心。访问鉴证中心比较它的 AUTHR 计算值和从移动站接收的值。如果这些值匹配，则鉴证出移动站并且允许该移动站接入访问网络。另外，移动站和访问鉴证中心计算密码本 K_C 的值，这里值 K_C 等于使用值 R_N 作为输入和值 SSDB 作为密钥输入的 CAVE 算法的输出。这时，允许移动站和访问网络之间的通讯并且可以使用密码函数加密这些通讯，这里密码函数的输入是要被加密的消息和密钥 K_C。密码函数由 CDMA 和 TDMA 系统它们各自的标准规定。应该注意对于 IS41，与每次对移动站的呼叫不同，仅仅每当移动站在访问网络登记时执行访问鉴证中心和归属鉴证中心之间的通讯。

上面讨论的方法说明了一种用于验证移动站被授权可以接入网络的方式，但是它们不涉及验证要求由一个合法网络识别自身的移动站。图 4 说明一个建议，用于对 IS41 标准的改进以允许访问网络和移动站之间相互鉴证。图 4 说明一旦移动站和访问位置寄存器接收到如上面关于图 3a 讨论的值 SSDA 和 SSDB 时的相互鉴证过程。访问网络通过发射随机数 R_N 询问移动站。移动站随后通过进行一个计算以获得使用值 R_N 和 R_M 作为输入和值 SSDA 作为密钥输入的密码函数 F^1 的输出而响应。在这种情况下，R_N 是由访问网络发射的相同值而值 R_M 是由移动站计算的随机数。除了发射这个密码函数的输出以外，值 R_M 也以未加密形式发射到访问网络。访问网络使用值 R_N 和 R_M 的未加密形式作为到 F^1 密码函数的输入以及值 SSDA 作为密钥输入计算 F^1 密码函数的输出。这个输出值与从移动站接收的值

相比较，如果它们匹配，则验证或鉴证出移动站。然后通过对移动站以值 R_M 形式提供的询问的响应由移动站鉴证或验证访问网络。访问鉴证中心随后发射使用值 R_M 作为输入和值 SSDA 作为密钥输入的密码函数 F^2 的输出。然后移动站进行相同的计算并且将它从访问网络接收的值与使用密钥值 SSDA 和值 R_M 的密码函数 F^2 的输出获得的值相比较。如果这些值匹配，移动站认为鉴证或验证了网络并且继续与该网络通讯。访问鉴证中心和移动站都通过获得使用值 R_N 和 R_M 作为输入和值 SSDB 作为密钥输入的密码函数 F^3 的输出来计算密码本 K_C 的值。这时，移动站和访问网络可以通讯；然而，如果要求加密通讯，则使用具有被加密消息作为输入和值 K_C 作为密钥输入的加密算法 F^4 加密这些消息。密码函数 F^1、F^2 和 F^3 可以是散列函数或一个如 SHA-1 的密码函数，而函数 F^4 可以是如 DES 的密码函数。散列函数、如 SHA-1 的单向密码函数和如 DES 的密码函数在本领域是公知的。

建议的相互鉴证过程具有效率低的缺点，这在于它要求在鉴证过程可以开始之前移动站和访问位置寄存器都具有值 SSDA 和 SSDB。因此，在移动站和访问鉴证中心之间至少要求两组通讯。第一组通讯提供给移动站用于计算值 SSDA 和 SSDB 的信息。第二组通讯用于实现相互鉴证。

本发明通过使用发射到终端的鉴证询问以提供给终端计算鉴证和密码本值的信息来提供一种用于实现鉴证的更有效的方法。因此，不要求分开的通讯来提供给终端密钥值，消除了两组通讯的低效率。访问鉴证中心从归属鉴证中心获得随机值 R_T、鉴证密钥值 K_A 和密码本值 K_C。访问鉴证中心随后发射随机数 R_T 到终端以更新终端的鉴证密钥和密码本值，并且询问终端作为鉴证过程的一部分。终端使用 R_T 计算鉴证密钥值 K_A 和密码本值 K_C 并且响应访问鉴证中心的询问。另外，鉴证密钥值用于验证访问网络对于终端鉴证询问网络的响应。

图 1 说明移动站、访问网络和归属网络之间的通讯。

图 2 说明对于 GSM 网络的鉴证过程。

图 3a 和 3b 说明对于 IS41 依从网络的密钥更新和鉴证过程;

图 4 说明一种建议的相互鉴证方法; 以及

图 5 说明一种用于实现密钥更新和相互鉴证的方法。

图 5 说明一种方法，这里发射到移动站或固定终端的单个随机值用于更新终端的鉴证和密码本值并且对于终端提供鉴证询问。移动站或固定终端 70 以及归属位置寄存器 72 共享密钥值 K_i。当移动终端 70 请求接入访问网络时，访问鉴证中心接触归属鉴证中心以获得随机值 R_T、鉴证密钥值 K_A 和密码本值 K_C。响应这种请求，归属鉴证中心使用如经过访问鉴证中心由移动终端提供的电话号码的识别码进入与移动终端 70 有关的归属位置寄存器 72。归属鉴证中心随后通过采用使用随机数 R_T 作为输入和值 K_i 作为密钥输入的密码函数 F^4 的输出计算鉴证密钥值 K_A。另外，归属鉴证中心使用将值 R_T 作为输入和值 K_i 作为密钥输入的加密函数 F^C 的输出计算密码本值 K_C。一旦计算出这些值，归属鉴证中心传递值 R_T、K_A 和 K_C 到访问鉴证中心。访问鉴证中心随后存储值 K_A、K_C 和 R_T 在与移动站终端 70 有关的访问位置寄存器。访问鉴证中心随后传递值 R_T 到移动站终端 70 作为鉴证询问和将用于更新由移动站终端使用的鉴证和密码本值的值。移动站终端使用从访问鉴证中心接收的值 R_T 以归属鉴证中心计算的值的相同方式计算鉴证密钥值 K_A 和密码本值 K_C。移动站终端随后使用鉴证密钥值 K_A 以响应访问鉴证中心的鉴证询问。移动站终端确定使用值 R_T 和 R_M 作为输入和鉴证密钥值 K_A 作为密钥输入的密码函数 F^1 的输出; 然而，也可能使用值 R_T 而不是 R_T 和 R_M 作为输入。密码函数 F^1 的输出和值 R_M 被传递到访问鉴证中心; 但是如果 R_M 不用作密码函数 F^1 的输入并且如果不请求网络的鉴证则值 R_M 可能不被发射。值 R_M 是一个由移动站终端选择的随机值。访问鉴证中心也计算具有输入 R_T 和 R_M 以及密钥输入值 K_A 的函数 F^1 的输出值使得该结果可以与移动站终端传递的值相比较。如果这些值匹配，则对于访问网络鉴证或验证出移动站终端。由移动站终端

提供的值 R_M 用作移动站 70 对访问网络的鉴证询问。访问网络计算使用值 R_M 作为输入和值 K_A 作为密钥输入的函数 F^2 的输出。这个输出值随后传递到移动站终端，这里终端独立地确定具有值 R_M 作为输入和值 K_A 作为密钥输入的函数 F^2 的输出。如果输出值匹配，则移动站终端验证或鉴证该访问网络 。一旦移动站终端和访问网络已经鉴证或验证出相互的身份，通讯可以继续。这个通讯可以使用未加密消息或加密消息进行。如果使用加密消息，则通过使用具有消息作为输入和密码本值 K_C 作为密钥输入的密码函数 F^2 的输出加密消息。每当在移动站终端和访问网络之间试图呼叫时可以执行这个过程。每当移动站登记访问网络而不是每次试图呼叫时也可能接触归属鉴证中心，并且只要移动站继续登记访问网络就使用相同的 K_A、K_C 和 R_T 值。密码函数 F^1、F^2、F^A 和 F^C 可以是散列函数或一个如 SHA-1 的密码函数，而函数 F^3 可以是如 DES 的密码函数。散列函数、如 SHA-1 的单向密码函数和如 DES 的密码函数在本领域是公知的。

当移动站终端在归属网络时也可能执行相同的过程。在这种情况下，归属鉴证中心而不是访问鉴证中心与移动站终端通讯。在无线网络中，在终端和鉴证中心之间的通讯经过无线基站。

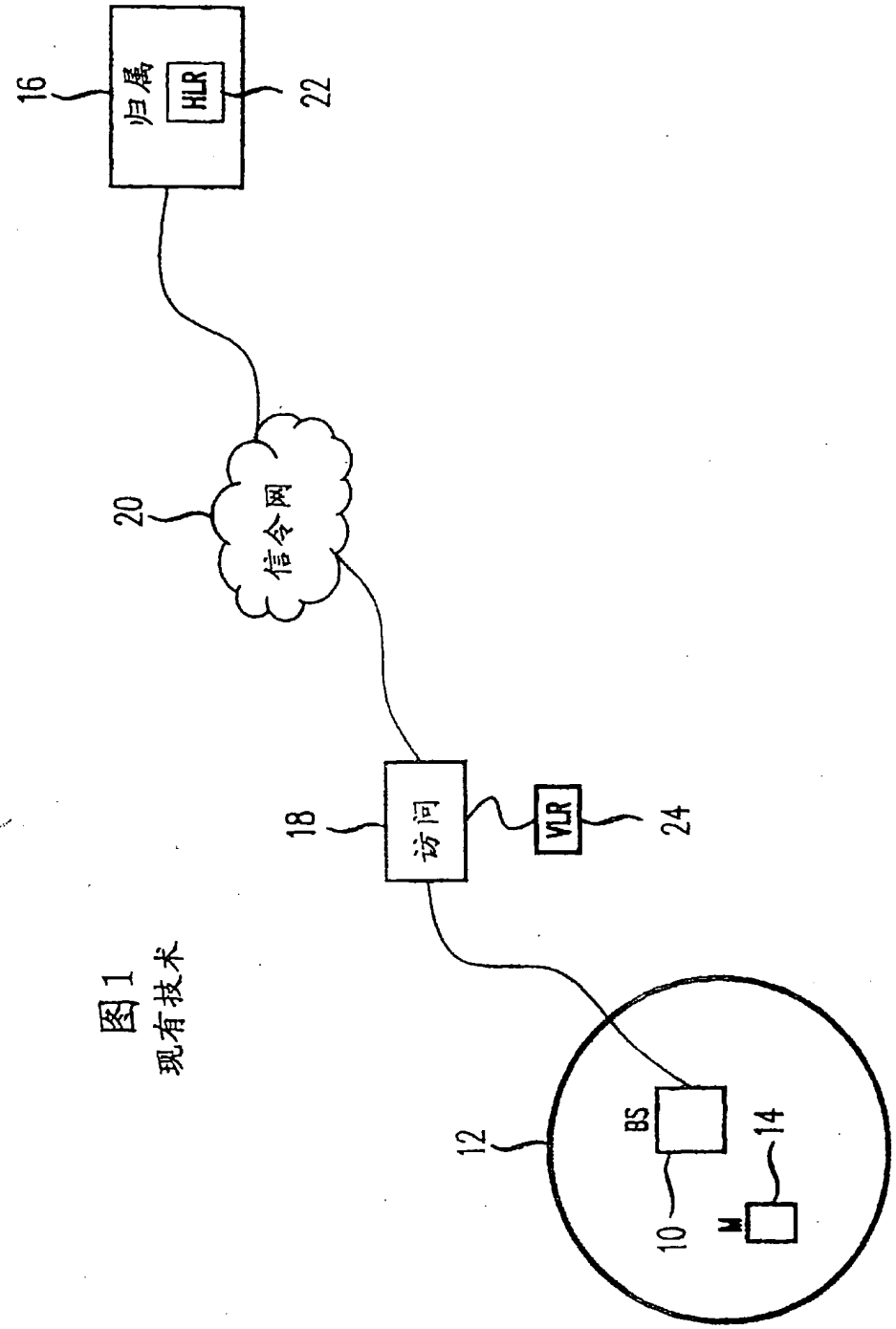


图 1
现有技术

图 2（现有技术）

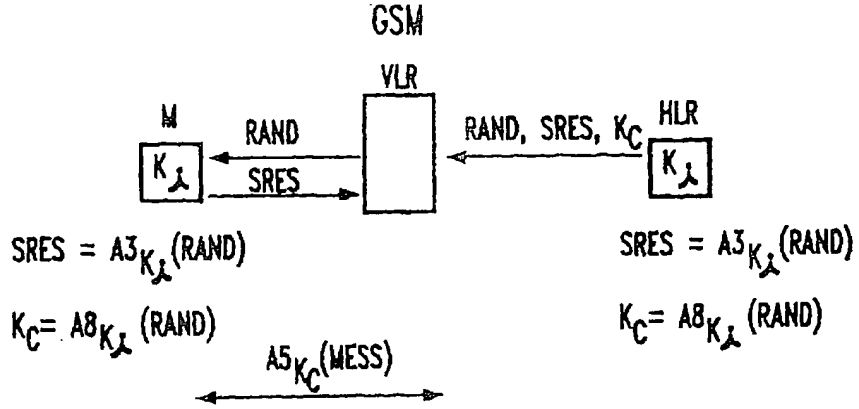


图 3A（现有技术）

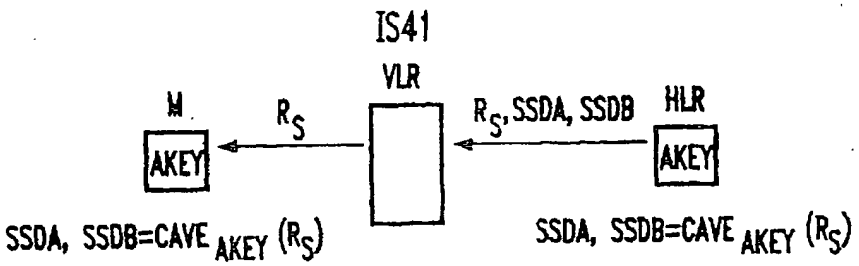


图 3B（现有技术）

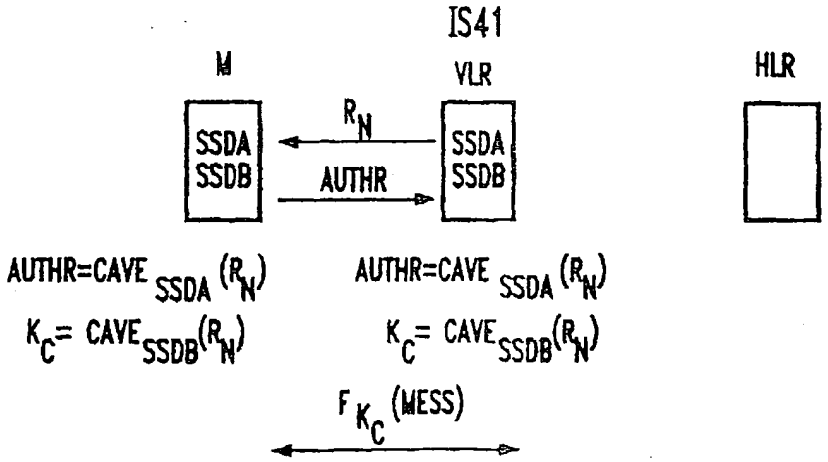


图4（现有技术）

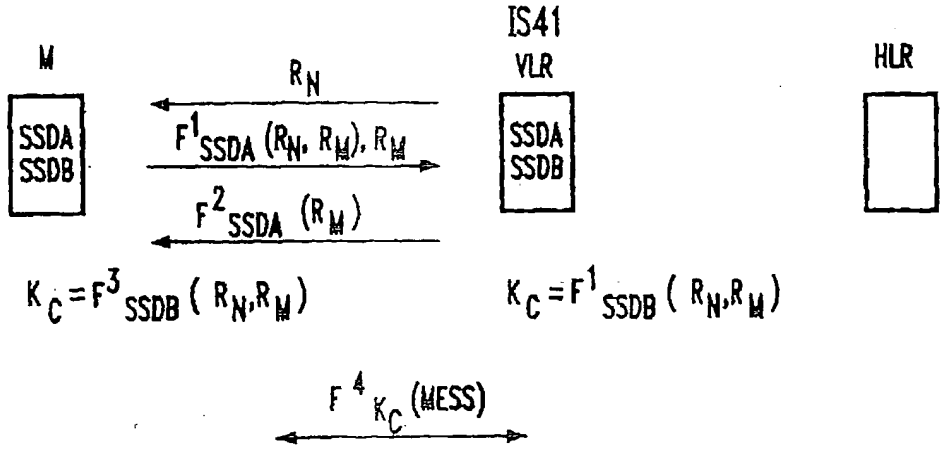
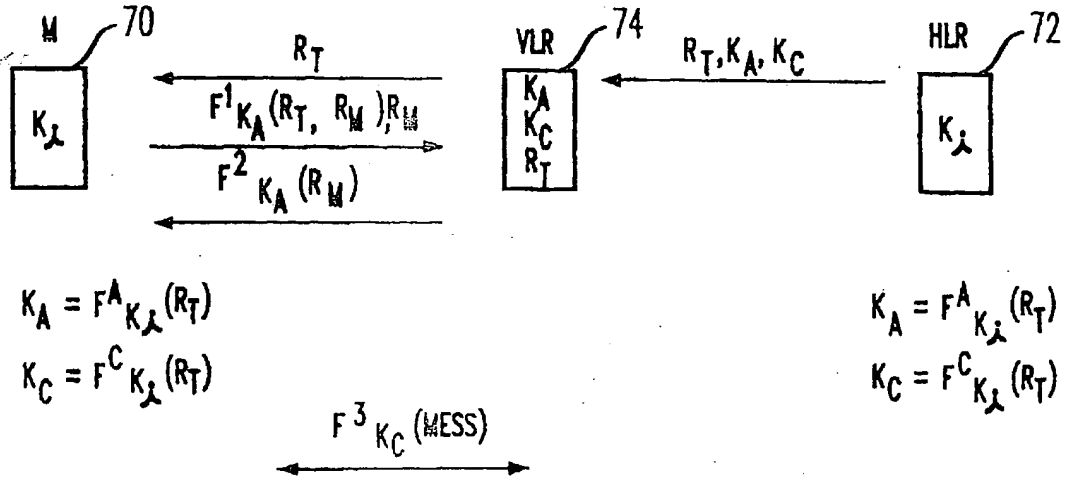

IS41
M
VLR
HLR
R_N
SSDA
SSDB
$F^1_{SSDA}(R_N, R_M), R_M$
$F^2_{SSDA}(R_M)$
SSDA
SSDB
$K_C = F^3_{SSDB}(R_N, R_M)$
$K_C = F^1_{SSDB}(R_N, R_M)$
$F^4_{K_C}(MESS)$

图5


M
70
VLR
74
HLR
72
R_T
R_T, K_A, K_C
K_i
K_A
K_C
R_T
K_i
$F^1_{K_A}(R_T, R_M), R_M$
$F^2_{K_A}(R_M)$
$K_A = F^A_{K_i}(R_T)$
$K_C = F^C_{K_i}(R_T)$
$K_A = F^A_{K_i}(R_T)$
$K_C = F^C_{K_i}(R_T)$
$F^3_{K_C}(MESS)$